**Темы курсовых работ по дисциплине**

**«Программирование алгоритмов защиты информации»**

**для студентов четвертого курса, 2019 год**

1. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Эдвардса с использованием библиотеки libcrypto.

2. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Монтгомери с использованием библиотеки libcrypto.

3. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Монтгомери с использованием библиотеки libcrypto.

4. Разработка загрузчика и виртуальной машины для языка программирования с защищенной средой выполнения.

5. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Монтгомери с использованием библиотеки libgcrypt.

6. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Эдвардса с использованием библиотеки libgcrypt.

7. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Якоби с использованием библиотеки libcrypto.

8. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Якоби с использованием библиотеки libcrypto.

9. Написание модуля упаковки PE файлов.

10. Реализация механизмов имитозащиты данных при их передаче с оконечного устройства (микроконтроллер) на центральное в сетях Интернета вещей.

11. Написание модуля шифрования упакованной структуры PE и ELF файлов.

12. Руководство по работе с микроконтроллером ESP8266. Реализация зашифрованного канала связи.

13. Разработка парсера и компилятора для языка программирования с защищенной средой выполнения.

14. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Эдвардса с использованием библиотеки gmp.

15. Анализ реализации протокола WPA3 в приложении ОС Linux wpa\_supplicant.

16. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Якоби с использованием библиотеки libakrypt.

17. Написание модуля упаковки ELF файлов.

18. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Якоби с использованием библиотеки libgcrypt.

19. Реализация функции хэширования Keccak с использованием библиотеки libakrypt.

20. Реализация эффективных алгоритмов вычисления кратной точки эллиптической кривой в форме Монтгомери с использованием библиотеки gmp.